Cracking the Code on

C-level Security Collaboration

Accenture Cybersecurity Forum
Global Executive Leadership Network

14 February 2023
Session Summary

From the ACF Chair

You put Accenture's CEO on the spot with your insightful questioning. She really enjoyed it.

Thanks to all those who participated in our roundtable discussion with Julie Sweet, Accenture's CEO and board chairperson. We appreciated the opportunity to address your questions and hear firsthand what's on your minds as CISOs. The feedback we've received from members was universally positive, but one suggestion Julie offered clearly stood out: **"Don't do a data dump on the board."**

We hope you find the ideas that emerged from the conversation useful as you lead your enterprise towards a more cybersecure, resilient future.

Cheers,
Kris Burkhardt
Accenture CISO, ACF Chair

LinkedIn: Kristian Burkhardt

Cracking the Code on C-level Security Collaboration

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “Cracking the Code on C-level Security Collaboration,” on February 14, 2023. CISOs face the challenge of securing the enterprise while also enabling the enterprise to operate effectively. Meeting these challenges requires CISOs to collaborate with the business, the C-suite and the board. For insight on effective collaboration, this session featured a conversation and Q&A with Julie Sweet, Accenture CEO and chairperson of the board of directors.

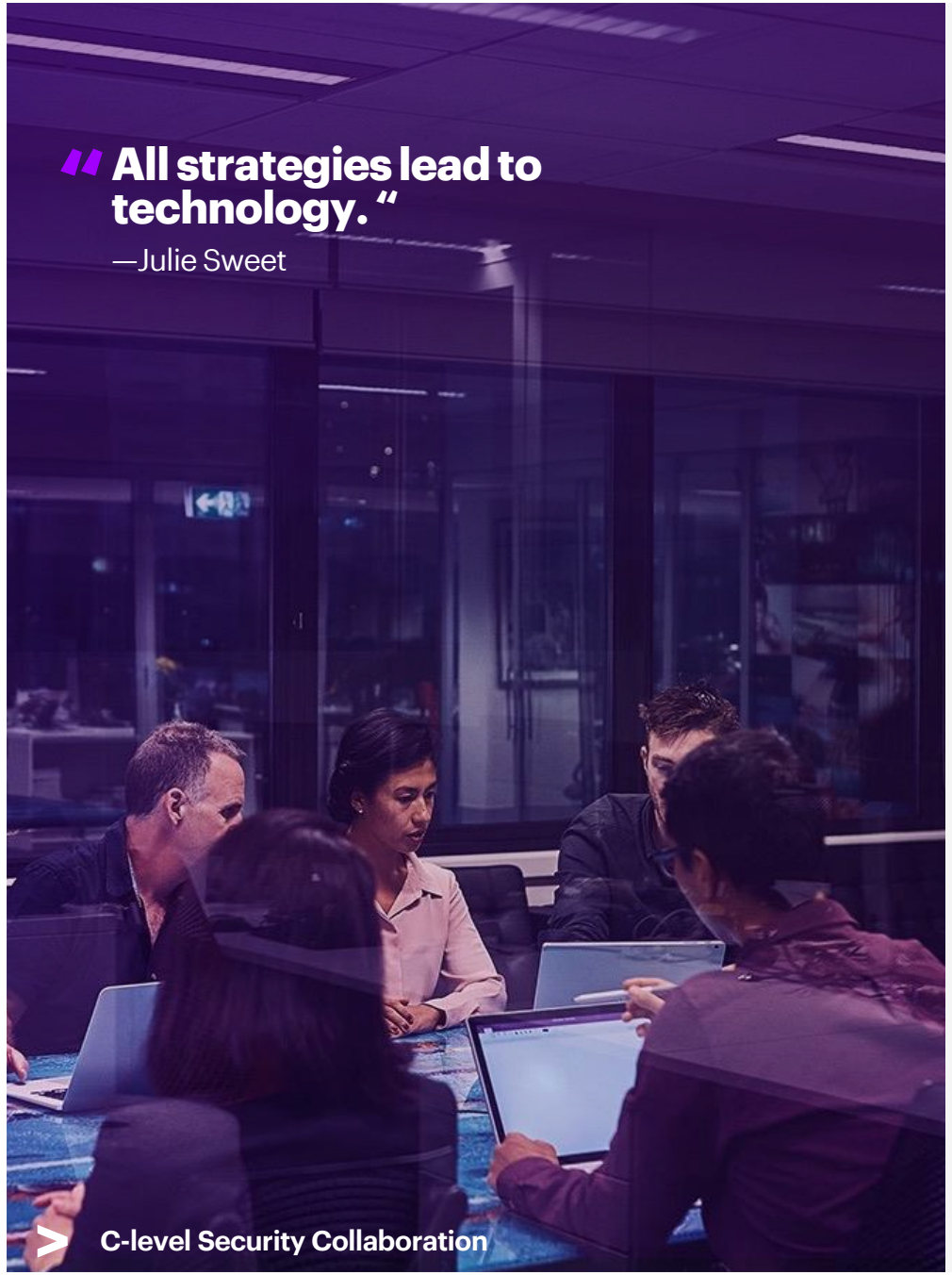
This roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers, nor participants, is revealed.

In this summary:

Davos highlights >

The challenge of creating a secure digital core

Leading practices for engaging with the board >



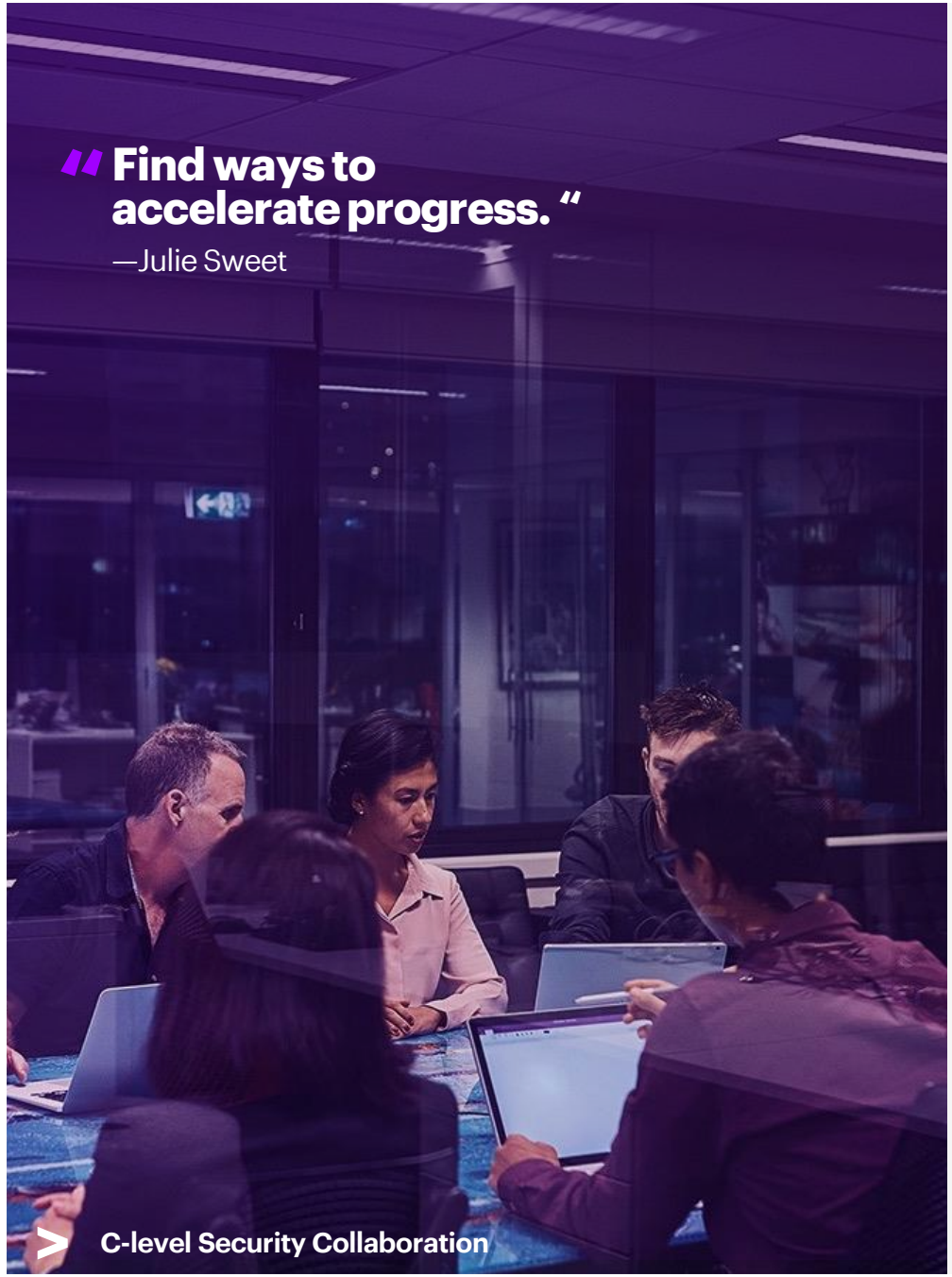
Davos highlights

Sweet noted that geopolitical concerns, particularly related to security, risks and new markets, were top of mind among the Davos participants. However, she also noted a greater sense of optimism than at past events even as the threat landscape is expanding. A message she shared with other Davos participants was that: “All strategies lead to technology. An enterprise’s ability to succeed is founded on its ability to change and is centered around a strong digital core that will enable industry-disrupting total enterprise reinvention.”

The challenge of creating a secure digital core

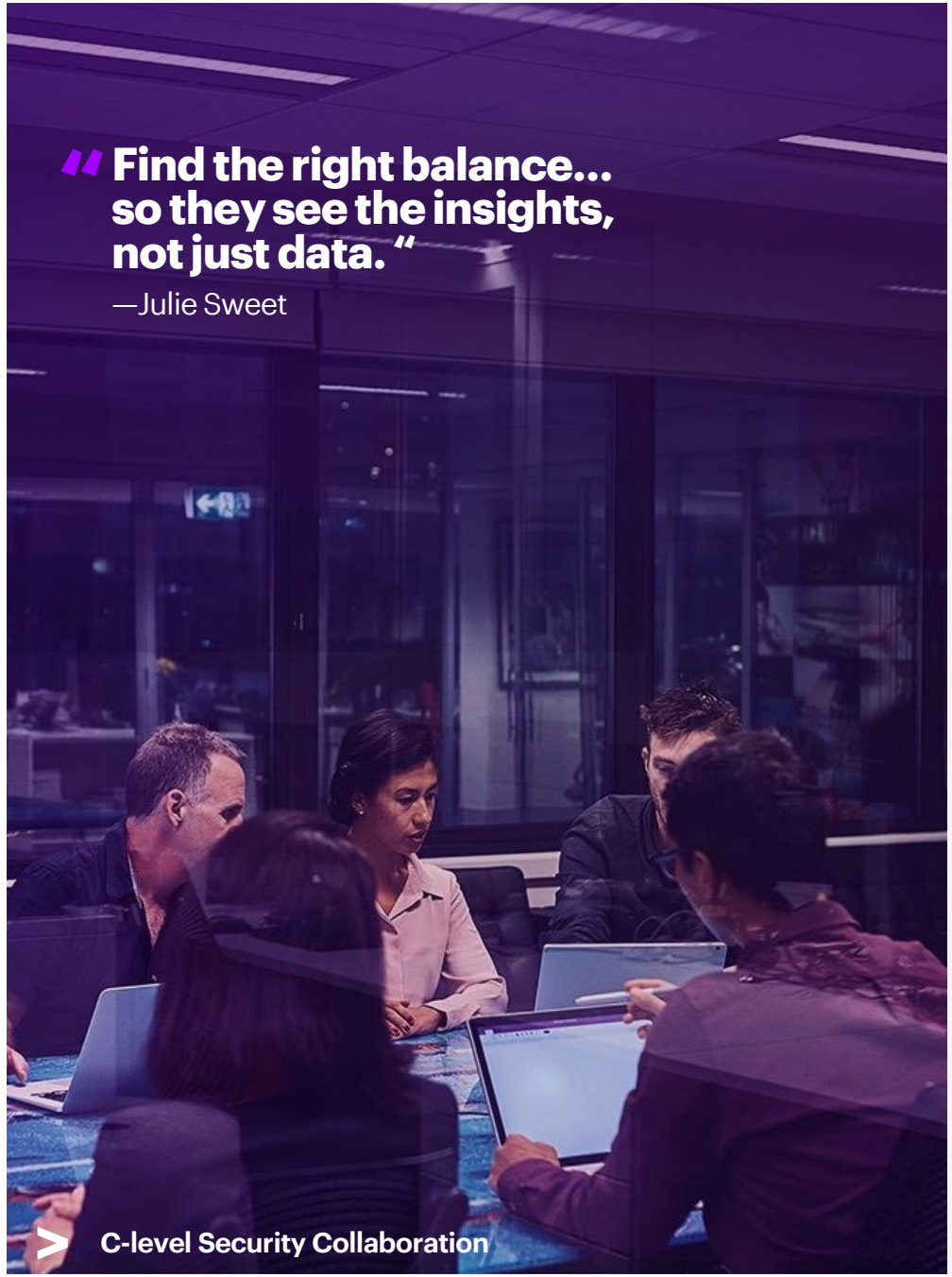
In her conversations with other CEOs and board members about total enterprise reinvention, Sweet sees common themes specific to cybersecurity.

- **Greater mindshare.** While total enterprise reinvention is gaining traction among CEOs, “Not enough mind share is devoted to cybersecurity unless the enterprise has recently experienced a breach,” said Sweet. She encouraged CISOs to help management teams focus on the security element of the digital core to the same extent they are concerned about generative AI headlines and cloud vendor selection.
- **Platform perspective.** While many enterprises are thinking about technology investments in terms of adaptable platforms and architecture, the same perspective on consolidation should be applied to security. The CEO should be asking the CISO: “Who are you partnering with? How many tools are you using? Where can we find efficiencies?”
- **Business metrics.** CEOs should set expectations that cybersecurity will be held to oversight similar to other functions. “Security should be evaluated at the same level as financial reporting,” Sweet said. The CISO needs to be transparent when there are issues and how they will be addressed. Metrics are particularly helpful in holding people accountable, Sweet said.
- **Multiple lenses.** Sweet said that boards are better informed about cybersecurity when they are exposed to multiple perspectives, for example from the CISO, the Enterprise Risk Management Lead and Internal Audit.



The challenge of creating a secure digital core (cont.)

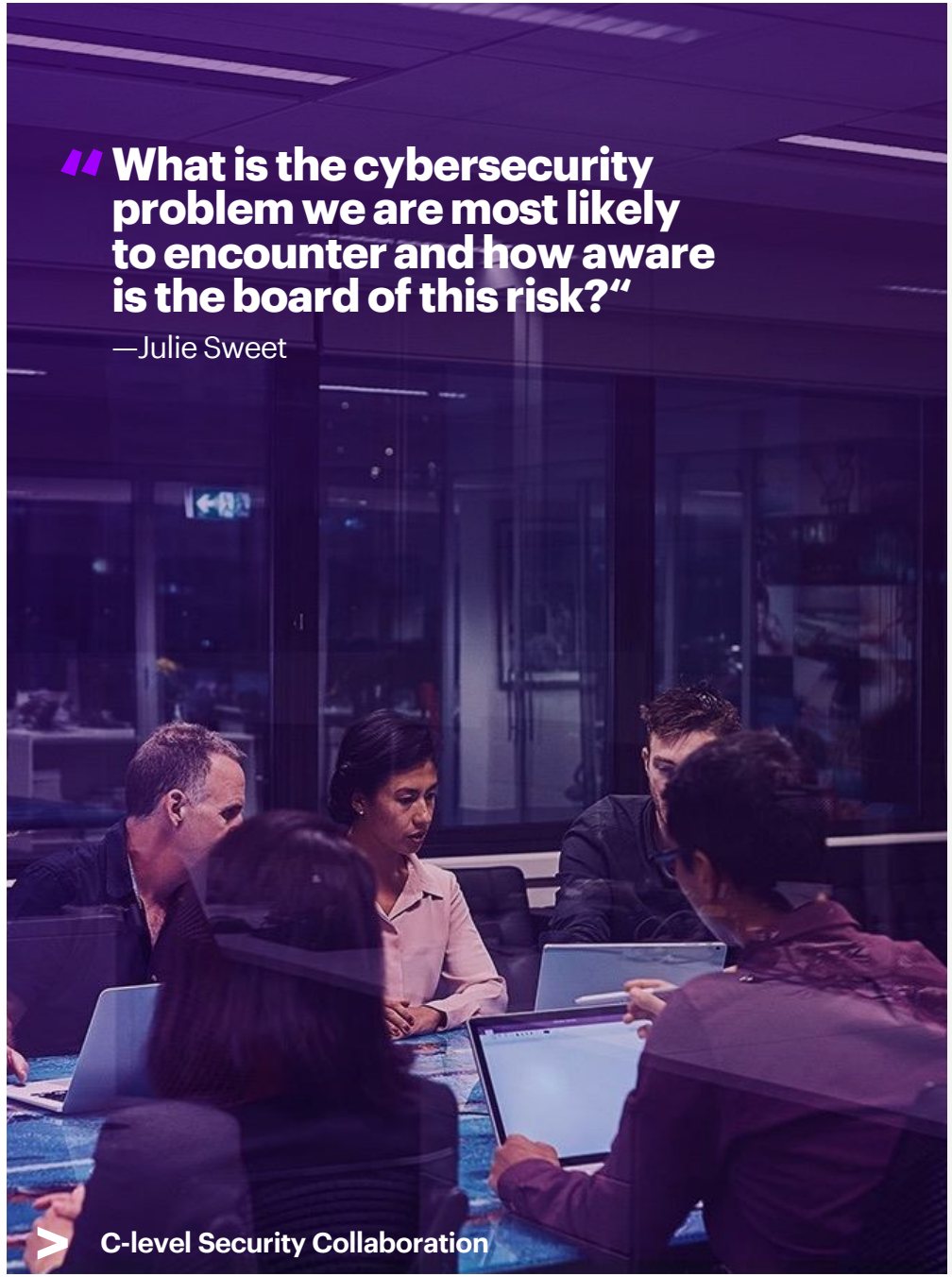
- **The emergence of AI.** Accenture is setting policies to ensure the responsible use of AI, including compliance requirements on par with other programs. For example, generative AI, such as ChatGPT cannot be used in conjunction with either Accenture or client data without explicit approval.
- **Avoid silos.** CEOs, with support from the CISO, should help other leaders make the connection between legacy systems and total enterprise reinvention initiatives. “Avoid separate cybersecurity discussions about legacy systems and digital core upgrades,” said Sweet.
- **Cyber as an enabler.** Cybersecurity can be an enabler of new products and services, Sweet said. For example, consumers want to know that their identity is protected and doing so can be a powerful selling point. As a CISO you can make a real contribution by engaging with the business on that issue.” A CISO offered another example. Because maintaining employee digital identity is simplified and ubiquitous, acquisitions can be integrated more quickly and safely and start creating value with greater velocity. Sweet added: “Onboarding can be painfully slow and the CISO doesn’t want to be a pain point that delays the process. Find ways to accelerate progress.”
- **The cyber talent shortage.** Sweet said that managed services are a particularly attractive alternative to recruiting and retaining cyber talent in house because accessing outside talent can accelerate digitization, keep the enterprise more resilient and enable more efficient spending.



Leading practices for engaging with the board

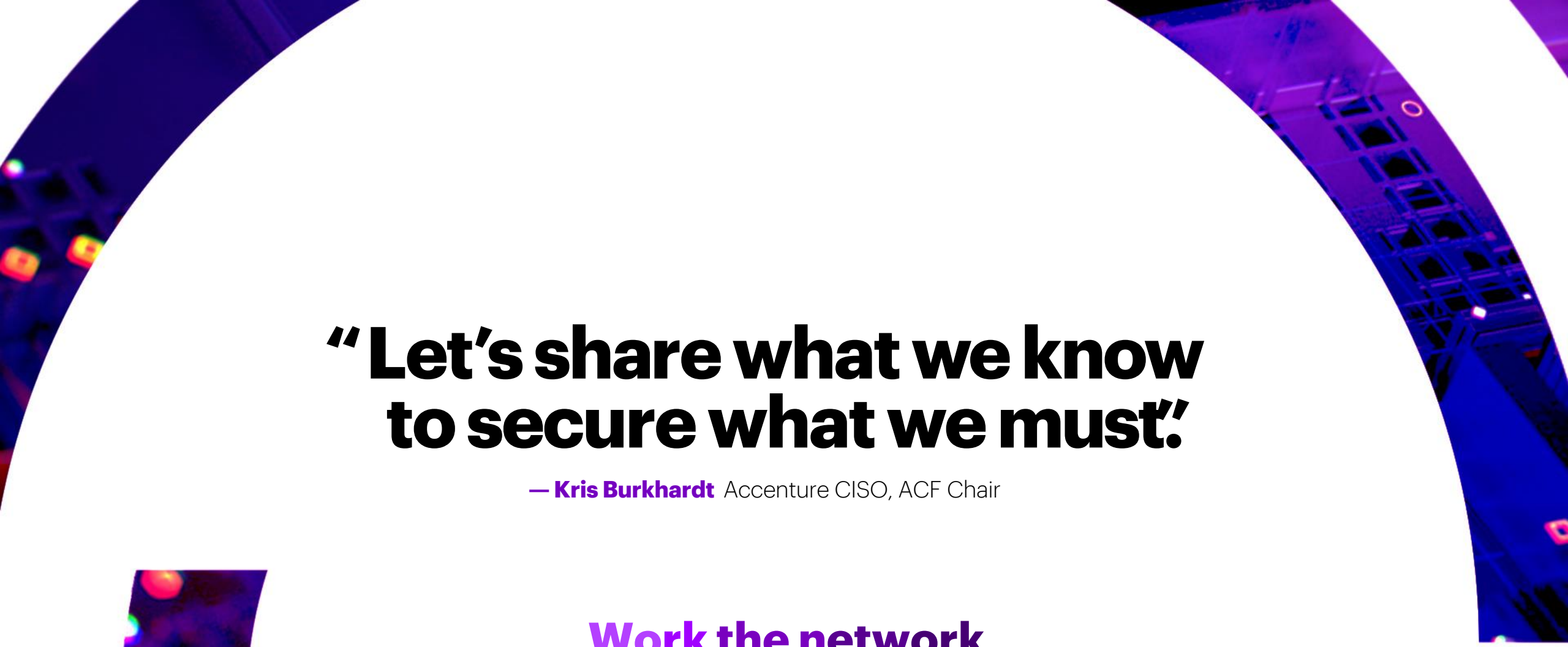
ACF members raised a variety of questions about how CISOs can communicate more effectively with the board of directors. Practical suggestions included:

- **Don’t overdo data.** “Avoid the data dump. Sometimes CISOs share too much data or a scorecard that is too dense. The board can’t see the forest for the trees,” Sweet said. “Find the right balance with your audience so they see the insights, not just data. Help them understand what the most important risks are, and how they should be thinking about them.”
- **Test your messages.** A CISO and the Accenture CEO both spoke about the value of testing messages with stakeholders, such as the head of the Audit Committee, before formal presentations. “I find it very useful to check in with our lead director,” said the CISO. Sweet suggested that as part of the annual collection of feedback from board members, consider including a specific question about how they perceive the quality of reporting on cybersecurity issues.



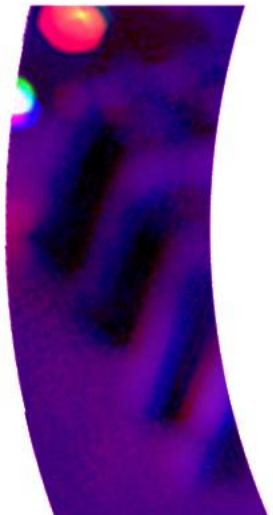
Leading practices for engaging with the board (cont.)

- **“No surprises.”** Well-prepared CISOs are asking themselves, “What is the cybersecurity problem we are most likely to encounter and how aware is the board of this risk?” Sweet said. Addressing that core question can help the board avoid surprises. ACF members also spoke about the challenge of board communications. Quoting George Bernard Shaw, a CISO said: "The single biggest problem in communication is the illusion that it has taken place.” A subject-matter expert added: “One-and-done crisis management exercises with the C-suite and the Board are insufficient. Doing them regularly—and showing continuous process improvement over time—is much more effective.”
- **The CISO as advisor.** Whether or not the management team understands cyber risks can be a function of how the CISO is positioned within the organization. “The CISO’s responsibilities as an advisor should be spelled out in the job description,” said an ACF member. Another added: “The CISO community overall needs to step up when it comes to assertive, business-centric communications if they expect to perform the advisory part of the job effectively.”



“Let’s share what we know to secure what we must.”

— **Kris Burkhardt** Accenture CISO, ACF Chair



Work the network

Contact our team directly
for questions and member introductions.

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Technology and Operations services and Accenture Song — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 721,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter, LinkedIn or visit us at accenture.com/security.